CLAIMS

1. A method of performing an inversion operation in a cryptographic calculation with at least two auxiliary variables, the method comprising shifting (S2) a variable, then effecting a reduction (S3) by subtracting that variable from a larger variable.

2. A method according to Claim 1 wherein the variables are of the same degree.

3. A method according to Claim 1 or 2 comprising updating a plurality of additional variables such that the invariances remain valid.

4. A method according to any preceding claim comprising four auxiliary variables being U, V, R and S, having the invariances:

$|S.V-R.U| = N$

$S.Y = U \bmod N$

$R.Y = V \bmod N$.

5. A method according to Claim 4 comprising decreasing U and V in size, step by step until $U = 1$.

6. A method according to Claim 5 comprising effecting the operation $R.Y = 1 \bmod N$ or $R = Y^{-1} \bmod N$, as appropriate.

7. A method according to any preceding claim comprising operating with the Most Significant Words of the variables.

8. A method according to any preceding claim comprising providing inversion (S1-S4) over GF(p).

9. A method according to any preceding claim comprising providing inversion (S10-S12) over GF(2^n).

10. A method according to any preceding claim comprising providing a method for long-integer division operations.

11. A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of any one or more of Claims 1 to 10 when said product is run on a computer.

12. A computer program directly loadable into the international memory of a digital computer, comprising software code portions for performing the method of any one of Claims 1 to 10 when said program is run on a computer.

13. A carrier, which may comprise electronic signals, for a computer program of Claim 12.

14. Electronic distribution of a computer program product of Claim 11 or a computer program of Claim 12 or a carrier of Claim 13.

15. Apparatus for performing an inversion operation in a cryptographic calculation with at least two auxiliary variables, the apparatus comprising means to shift a variable (V, R) and means (10-17) to effect a reduction by subtraction or addition of that variable from a larger variable.

16. Apparatus according to Claim 15 wherein the variables (V, R) are of the same degree without shifting.

17. Apparatus according to Claim 15 or 16 comprising means to update a plurality of additional variables such that the invariance remains valid.

18. Apparatus according to any of Claims 15 to 17 comprising means (10-13) to operate four auxiliary variables being U, V, R and S, having the invariances:

$|S.V-R.U| = N$

$S.Y = U \bmod N$

$R.Y = V \bmod N.$

19. Apparatus according to Claim 18 comprising means (10, 11) to decrease U and V in size, step by step until U = 1.

20. Apparatus according to Claim 19 comprising means (10-16) to effect the operation $R.Y = 1 \bmod N$ or $R = Y^{-1} \bmod N$, as appropriate.

21. Apparatus according to any of Claims 15 to 20 comprising means to operate with the Most Significant Words of the variables.

22. Apparatus for performing an inversion operation in a cryptographic calculation substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of the Figures of the accompanying drawings.

23. A method of performing an inversion operation in a cryptographic calculation substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of the Figures of the accompanying drawings.